

What is claimed is:

1 1. A system for providing secure exchange of sensitive information
2 with an implantable medical device, comprising:
3 a crypto key uniquely associated with an implantable medical device to
4 encrypt sensitive information during a data exchange session; and
5 an external source to securely obtain the crypto key over a secure
6 connection from a secure key repository securely maintaining the crypto key, to
7 encrypt the sensitive information using the crypto key and to store the sensitive
8 information as encrypted data onto the implantable medical device.

1 2. A system according to Claim 1, further comprising:
2 a short range interface to logically define a secured area around the
3 implantable medical device within which to securely obtain the crypto key; and
4 a long range interface to logically define a non-secured area extending
5 beyond the secured area within which to exchange the encrypted data.

1 3. A system according to Claim 1, wherein the encrypted data is
2 retrieved from the implantable medical device over a non-secure connection and
3 the encrypted data is decrypted as the sensitive data using the crypto key.

1 4. A system according to Claim 3, wherein the crypto key is securely
2 retrieved over a secure connection from the secure key repository prior to
3 decrypting the encrypted data.

1 5. A system according to Claim 3, wherein the encrypted data is
2 retrieved through long range telemetry.

1 6. A system according to Claim 5, wherein the long range telemetry
2 comprises radio frequency telemetry.

1 7. A system according to Claim 1, wherein at least part of the
2 sensitive information is securely stored as unencrypted data onto the implantable
3 medical device over a secure connection.

1 8. A system according to Claim 7, wherein the unencrypted data is
2 securely retrieved from the implantable medical device over a secure connection.

1 9. A system according to Claim 1, wherein the crypto key is securely
2 retrieved from the secure key repository through a programmer.

1 10. A system according to Claim 1, wherein the crypto key is
2 maintained on the implantable medical device, and the crypto key is retrieved
3 through short range telemetry.

1 11. A system according to Claim 10, wherein the short range telemetry
2 comprises inductive telemetry.

1 12. A system according to Claim 1, wherein the external source
2 comprises at least one of a programmer and a repeater.

1 13. A system according to Claim 1, wherein the crypto key comprises
2 an encryption key in accordance with the Advanced Encryption Standard.

1 14. A method for providing secure exchange of sensitive information
2 with an implantable medical device, comprising:
3 defining a crypto key uniquely associated with an implantable medical
4 device to encrypt sensitive information during a data exchange session;
5 securely obtaining the crypto key over a secure connection from a secure
6 key repository securely maintaining the crypto key; and
7 encrypting the sensitive information using the crypto key and storing the
8 sensitive information as encrypted data onto the implantable medical device.

1 15. A method according to Claim 14, further comprising:
2 logically defining a secured area around the implantable medical device
3 within which to securely obtain the crypto key; and
4 logically defining a non-secured area extending beyond the secured area
5 within which to exchange the encrypted data.

1 16. A method according to Claim 14, further comprising:

2 retrieving the encrypted data from the implantable medical device over a
3 non-secure connection; and
4 decrypting the encrypted data as the sensitive data using the crypto key.

1 17. A method according to Claim 16, further comprising:
2 securely retrieving the crypto key over a secure connection from the
3 secure key repository prior to decrypting the encrypted data.

1 18. A method according to Claim 16, further comprising:
2 retrieving the encrypted data through long range telemetry.

1 19. A method according to Claim 18, wherein the long range telemetry
2 comprises radio frequency telemetry.

1 20. A method according to Claim 14, further comprising:
2 securely storing at least part of the sensitive information as unencrypted
3 data onto the implantable medical device over a secure connection.

1 21. A method according to Claim 20, further comprising:
2 securely retrieving the unencrypted data from the implantable medical
3 device over a secure connection.

1 22. A method according to Claim 14, wherein the crypto key is
2 securely retrieved from the secure key repository through a programmer.

1 23. A method according to Claim 14, further comprising:
2 maintaining the crypto key on the implantable medical device; and
3 retrieving the crypto key through short range telemetry.

1 24. A method according to Claim 23, wherein the short range
2 telemetry comprises inductive telemetry.

1 25. A method according to Claim 14, wherein the external source
2 comprises at least one of a programmer and a repeater.

1 26. A method according to Claim 14, wherein the crypto key
2 comprises an encryption key in accordance with the Advanced Encryption
3 Standard.

1 27. An apparatus for securely transacting a data exchange session with
2 an implantable medical device, comprising:
3 means for defining a crypto key uniquely associated with an implantable
4 medical device to encrypt sensitive information during a data exchange session;
5 means for securely obtaining the crypto key over a secure connection from
6 a secure key repository securely maintaining the crypto key; and
7 means for encrypting the sensitive information using the crypto key and
8 means for storing the sensitive information as encrypted data onto the implantable
9 medical device.

1 28. An implantable medical device for securely maintaining sensitive
2 information, comprising:
3 an implantable medical device, comprising:
4 a memory to store sensitive information encrypted using a crypto
5 key uniquely associated with an implantable medical device; and
6 a secure interface to provide access to the stored sensitive
7 information exclusively over a secure connection.

1 29. A method for securely maintaining sensitive information on an
2 implantable medical device, comprising:
3 storing sensitive information encrypted using a crypto key uniquely
4 associated with an implantable medical device; and
5 providing access to the stored sensitive information exclusively over a
6 secure connection.

1 30. An apparatus for securely maintaining sensitive information on an
2 implantable medical device, comprising:

- 3 means for storing sensitive information encrypted using a crypto key
- 4 uniquely associated with an implantable medical device; and
- 5 means for providing access to the stored sensitive information exclusively
- 6 over a secure connection.